

Internet of Things – Chancen nutzen und Risiken bewältigen mit Controlware

Dietzenbach, 06. Oktober 2020 – Internet of Things (IoT): Die Vernetzung physischer Objekte und deren Abbildung in der digitalen Welt eröffnen eine Vielzahl neuer technologischer Möglichkeiten. Unternehmen erschließen sich hier enorme Wachstumschancen, gleichzeitig entstehen aber auch neue Sicherheitsrisiken, denen die Netzwerke gewachsen sein müssen. Software Defined Networking (SDN) – ein zukunftsweisendes Netzwerkkonzept – ist die Basis, Ansprüchen an die digitalen Wertschöpfungsketten und das IoT sowie den gestiegenen Security-Anforderungen gerecht zu werden. Der Systemintegrator und Managed Service Provider Controlware unterstützt bei der Konzeption und Realisierung moderner und sicherer Netzwerke.

IoT-Infrastrukturen sind die Basis für durchgängig digital gesteuerte Prozesse in Unternehmen. Daten, die ursprünglich lediglich in nicht-digitaler Form zur Verfügung standen, lassen sich mit IoT digitalisieren und für die weitere Verarbeitung flexibel nutzbar machen. Bei den zur Anbindung an IP-basierte Netzwerke benötigten Geräten handelt es sich um Sensoren und Aktoren. Bisher in analoger Form vorliegende Daten erfahren durch die Umsetzung von IoT-Infrastrukturen eine sofortige Abbildung als sogenannter digitaler Zwilling und können nahtlos in automatisierte Prozesse integriert werden. Der Vorteil: Daten, die früher aufwendig – teilweise manuell – ermittelt, transformiert und modelliert wurden, stehen nun sofort zur Verfügung, um verarbeitet zu werden. Das eröffnet neue technologische Möglichkeiten, verändert Geschäftsmodelle in der Industrie und transformiert die Gesellschaft ins digitale Zeitalter.

Sichere Netzwerke

Allerdings müssen sich mit IoT auch die Sicherheitsarchitekturen der Netzwerke verändern: In der Vergangenheit reichte es in der Regel aus, die IT-Netzwerke am Zugang des Unternehmens über Firewalls und auf den Client-Systemen zu sichern. „Mittlerweile macht es die Einbindung von IoT-Geräten in die Netzwerke erforderlich, sich gegen Angriffe aus dem Netzwerk heraus – also von innen – abzusichern“, sagt Jens Müller, Senior Business Development Manager Network Solutions von Controlware. Darüber hinaus erfordert die Vielzahl der Systeme und ihre



unterschiedlichen Ausprägungen einen automatisierten Prozess, um einen geregelten Zugang zum Netzwerk zu ermöglichen – ohne dabei den Überblick zu verlieren.

„Über das Zugangsmanagement mit Network Access Control-Systemen (NAC) hinaus muss auch das Verkehrsverhalten von IoT-Endgeräten beobachtet werden“, so Jens Müller. Der Grund: In der Vergangenheit legten IT-Abteilungen ihren Fokus auf unternehmenseigene Geräte (Notebooks, PCs etc.), was Hackern nicht verborgen blieb. So wurden häufig ungeschützte IoT-Geräte (wie IP-fähige Thermostate, Video-Kameras, Aktoren der Hausautomation) innerhalb des Netzwerks zum Ausgangspunkt für Attacken auf das Unternehmen. Deshalb ist es wichtig, die Kommunikationsbeziehungen aller IT-Systeme und IoT-Komponenten zu überwachen. Jens Müller erklärt: „Bei plötzlich auftretenden anormalen Verkehrsbeziehungen oder massiv ansteigendem Datenverkehr von Clients ist es somit möglich, den jeweils betroffenen Client sofort vom Netzwerk zu trennen – beispielsweise über ein Quarantäne-Netz.“

Sicher mit Software Defined Networking

IoT erfordert neue, agile und sichere Netzwerke, was unbedingt innerhalb der betrieblichen Abläufe zu berücksichtigen ist. Software Defined-Netzwerke werden sowohl den Ansprüchen an digitale Wertschöpfungsketten und IoT als auch den gestiegenen Sicherheitsanforderungen gerecht. Diese Netze zeichnen sich durch stark automatisierte Betriebsabläufe aus. Durch Analytics wird die Administration, unter anderem beim Troubleshooting, deutlich vereinfacht. Ebenso unterstützen die durch SDN-Konzepte etablierten Strukturen die digitalen Geschäftsmodelle durch höhere Anpassungsgeschwindigkeiten – und sorgen netzübergreifend für die Abbildung der unternehmensweiten Sicherheitsanforderungen.

(4.019 Zeichen inkl. Leerzeichen)

Über Controlware GmbH

Die Controlware GmbH, Dietzenbach, ist einer der führenden unabhängigen Systemintegratoren und Managed Service Provider in Deutschland. Das 1980 gegründete Unternehmen entwickelt, implementiert und betreibt anspruchsvolle IT-Lösungen für die Data Center-, Enterprise- und Campus-Umgebungen seiner Kunden. Das Portfolio erstreckt sich von der Beratung und Planung über Installation und Wartung bis hin zu Management, Überwachung und Betrieb von Kundeninfrastrukturen durch das firmeneigene ISO 27001-zertifizierte Customer Service Center.



Zentrale Geschäftsfelder der Controlware sind die Bereiche Network Solutions, Collaboration, Information Security, Application Delivery, Data Center & Cloud sowie IT-Management. Controlware arbeitet eng mit national und international führenden Herstellern zusammen und verfügt bei den meisten dieser Partner über den höchsten Zertifizierungsgrad. Das rund 840 Mitarbeiter starke Unternehmen unterhält ein flächendeckendes Vertriebs- und Servicenetz mit 16 Standorten in DACH. Im Bereich der Nachwuchsförderung kooperiert Controlware mit renommierten deutschen Hochschulen und betreut durchgehend um die 50 Auszubildende und Studenten. Zu den Unternehmen der Controlware Gruppe zählen die Controlware GmbH, die ExperTeach GmbH, die Networkers AG und die productware GmbH.

Pressekontakt:

Stefanie Zender
Controlware GmbH
Tel.: +49 6074 858-246
Fax: +49 6074 858-220
E-Mail: stefanie.zender@controlware.de
www.controlware.de (Homepage)

fischerAppelt
Robert Schwarzenböck, Raphaela Sailer
Tel.: +49-89-747466-23
E-Mail: controlware@fischerappelt.de

